



# シナリオ : IPsec リモートアクセス VPN 設定

この章では、適応型セキュリティ アプライアンスを使用して、リモートアクセス IPsec VPN 接続を受け入れる方法について説明します。リモートアクセス VPN を使用すると、インターネットを越えてセキュアな接続（トンネル）を作成でき、オフサイトのユーザにセキュアなアクセスを提供できます。

Easy VPN ソリューションを実装する場合、この章では、Easy VPN サーバ（別名、ヘッドエンドデバイス）を設定する方法について説明します。

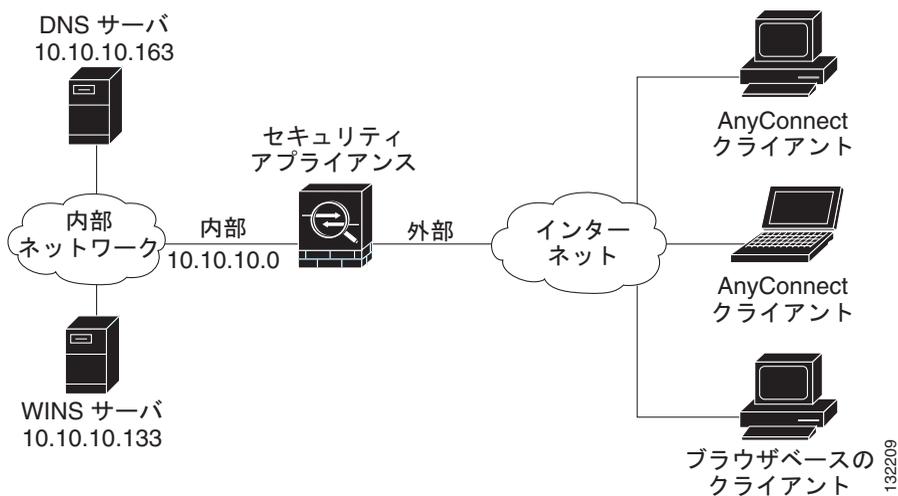
この章には、次の項があります。

- [IPsec リモートアクセス VPN ネットワーク トポロジの例 \(7-2 ページ\)](#)
- [IPsec リモートアクセス VPN シナリオの実装 \(7-3 ページ\)](#)
- [次の作業 \(7-24 ページ\)](#)

## IPsec リモートアクセス VPN ネットワーク トポロジの例

図 7-1 に、インターネットを越えて Cisco Easy VPN ソフトウェア クライアントまたはハードウェア クライアントなどの VPN クライアントからの要求を受け入れ、VPN クライアントとの IPsec 接続を確立するように設定された適応型セキュリティ アプライアンスを示します。

図 7-1 リモート アクセス VPN シナリオのネットワーク レイアウト



132209

## IPsec リモートアクセス VPN シナリオの実装

ここでは、リモート クライアントおよびデバイスから IPsec VPN 接続を受け入れるように適応型セキュリティ アプライアンスを設定する方法について説明します。Easy VPN ソリューションを実装する場合、この項では、Easy VPN サーバ (別名、ヘッドエンド デバイス) を設定する方法について説明します。

設定内容の例で使われる値は、[図 7-1](#) に示すリモートアクセス シナリオのもので

この項は、次の内容で構成されています。

- [収集する情報 \(7-4 ページ\)](#)
- [ASDM の起動 \(7-4 ページ\)](#)
- [IPsec リモートアクセス VPN 用の ASA 5505 の設定 \(7-6 ページ\)](#)
- [VPN クライアント タイプの選択 \(7-7 ページ\)](#)
- [VPN トンネル グループ名と認証方式の指定 \(7-9 ページ\)](#)
- [ユーザ認証方式の指定 \(7-11 ページ\)](#)
- [\(オプション\) ユーザ アカウントの設定 \(7-13 ページ\)](#)
- [アドレス プールの設定 \(7-14 ページ\)](#)
- [クライアント アトリビュートの設定 \(7-16 ページ\)](#)
- [IKE ポリシーの設定 \(7-18 ページ\)](#)
- [IPsec Encryption パラメータ および Authentication パラメータの設定 \(7-19 ページ\)](#)
- [アドレス変換の例外およびスプリット トンネリングの指定 \(7-20 ページ\)](#)
- [リモートアクセス VPN 設定の確認 \(7-22 ページ\)](#)

## 収集する情報

リモートアクセス IPsec VPN 接続を受け入れるように適応型セキュリティアプライアンスを設定する手順を開始する前に、次の情報を手元に用意してください。

- IP プールで使用する IP アドレスの範囲。これらのアドレスは、正常に接続されると、リモート VPN クライアントに割り当てられます。
- ローカル認証データベースを作成するときに使用するユーザのリスト (認証用に AAA サーバを使用している場合を除く)。
- VPN に接続する場合に、リモート クライアントが使用するネットワーク情報。内容は次のとおりです。
  - プライマリおよびセカンダリの DNS サーバの IP アドレス
  - プライマリおよびセカンダリの WINS サーバの IP アドレス
  - デフォルトのドメイン名
  - 認証されたリモート クライアントにアクセスできるローカル ホスト、グループ、およびネットワークの IP アドレスのリスト

## ASDM の起動

Web ブラウザで ASDM を実行するには、アドレス フィールドに工場出荷時のデフォルト IP アドレス **https://192.168.1.1/admin/** を入力します。



**(注)** 「https」の「s」を付け忘れると、接続は失敗します。HTTP over SSL (HTTPS) を使用すると、ブラウザと適応型セキュリティアプライアンスとの間の安全な接続が可能になります。

メイン ASDM ウィンドウが表示されます。

The screenshot displays the Cisco ASDM 5.2 web interface for a Security Appliance. The main content area is divided into several sections:

- Device Information:** Shows host name 'SecurityAppliance1', ASA version '7.2(0)72', device uptime '1d 1h 48m 24s', ASDM version '5.2(0)30', device type 'ASA/PIX', firewall mode 'Routed', context mode 'Single', total flash '64 MB', and total memory '512 MB'.
- VPN Status:** Shows 0 IKE Tunnels, 0 WebVPN Tunnels, and 0 SVC Tunnels.
- System Resources Status:** Includes CPU usage (0%) and memory usage (68MB) graphs.
- Interface Status:** A table showing the status of interfaces:
 

Interface	IP Address/Mask	Line	Link	Kbps
dmz	10.30.30.1/24		down	0
inside	10.10.10.1/24		down	0
management	172.23.62.22/24		up	5
outside	209.165.200.225/24		down	0
- Traffic Status:** Shows 'Connections Per Second Usage' and 'outside' Interface Traffic Usage (Kbps) graphs. The traffic usage graph indicates that the interface is down.

The status bar at the bottom shows 'Device configuration loaded successfully.', the user 'admin', and the time '5/10/06 1:08:18 AM PDT'.

153981

## IPsec リモートアクセス VPN 用の ASA 5505 の設定

リモートアクセス VPN の設定用のプロセスを開始するには、次の手順に従います。

- ステップ 1** ASDM メイン ウィンドウで、Wizards ドロップダウン メニューから **VPN Wizard** を選択します。VPN Wizard Step 1 画面が表示されます。



163910

**ステップ 2** VPN Wizard の Step 1 で、次の手順に従います。

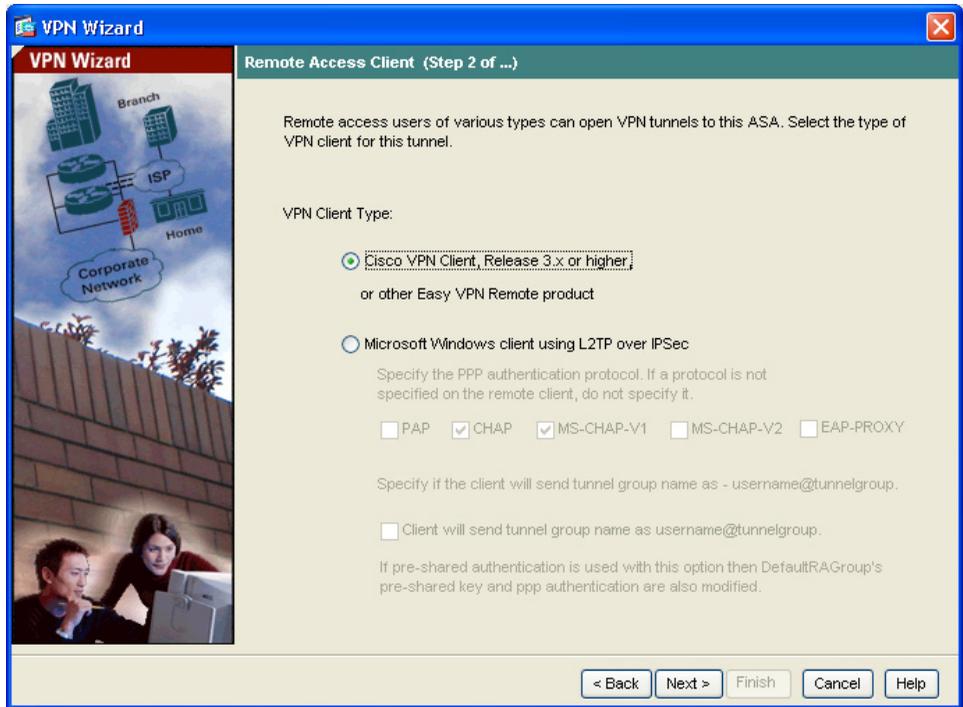
- a. **Remote Access** オプション ボタンをクリックします。
  - b. ドロップダウン リストから、着信 VPN トンネルで有効なインターフェイスとして **Outside** を選択します。
  - c. **Next** をクリックして続行します。
- 

## VPN クライアント タイプの選択

VPN Wizard の Step 2 で、次の手順に従います。

**ステップ 1** この適応型セキュリティ アプライアンスに接続するリモート ユーザを有効にする VPN クライアントのタイプを指定します。このシナリオでは、**Cisco VPN Client** オプション ボタンをクリックします。

その他の Cisco Easy VPN リモート製品も使用できます。



**ステップ 2** Next をクリックして続行します。

## VPN トンネル グループ名と認証方式の指定

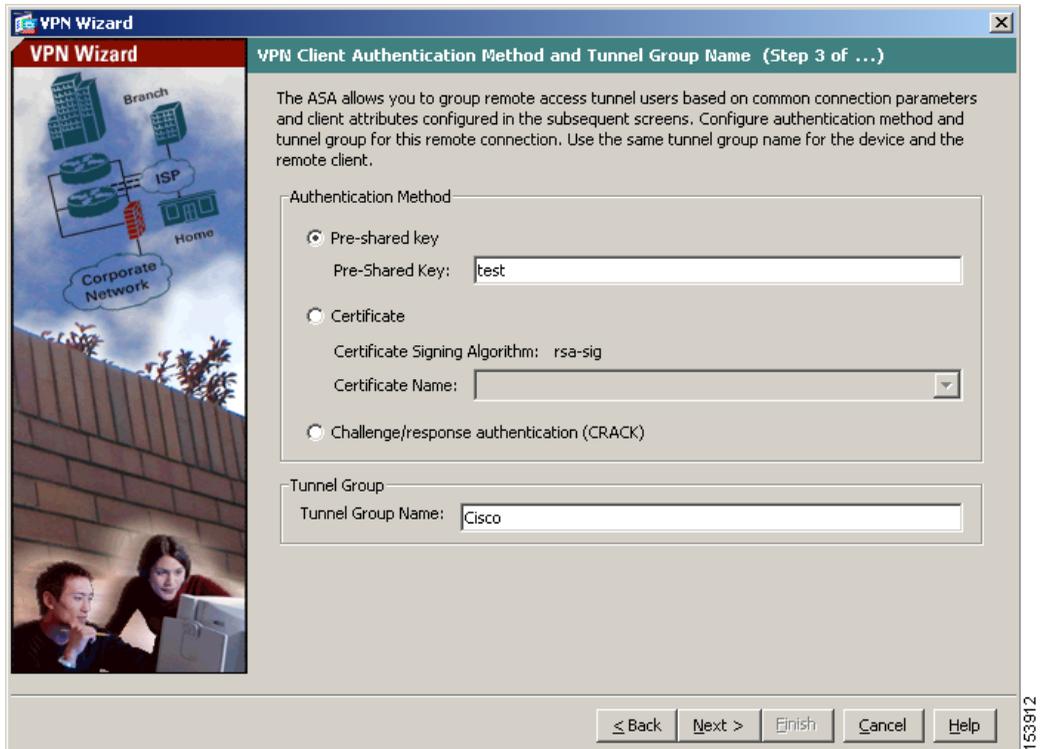
VPN Wizard の Step 3 で、次の手順に従います。

**ステップ 1** 次のいずれかの操作を実行して、使用する認証のタイプを指定します。

- 認証にスタティック事前共有キーを使用するには、**Pre-Shared Key** オプション ボタンをクリックし、事前共有キー（たとえば、「Cisco」）を入力します。このキーは、適応型セキュリティ アプライアンス間の IPSec ネゴシエーションで使用されます。
- 認証にデジタル証明書を使用するには、**Certificate** オプション ボタンをクリックし、ドロップダウン リストから証明書署名アルゴリズムを選択し、次に、事前設定されているトラストポイント名をドロップダウン リストから選択します。

認証にデジタル証明書を使用する予定で、まだトラストポイント名を設定していない場合は、他の 2 つのオプションのいずれかを使用してウィザードを続行できます。認証設定は、標準 ASDM ウィンドウを使用して後で修正できます。

- **Challenge/Response Authentication (CRACK)** オプション ボタンをクリックすると、この認証方式を使用できます。



**ステップ 2** 共通の接続パラメータおよびクライアント アトリビュートを使用して、この適応型セキュリティ アプライアンスに接続する複数ユーザのセットのトンネルグループ名（たとえば、「Cisco」）を入力します。

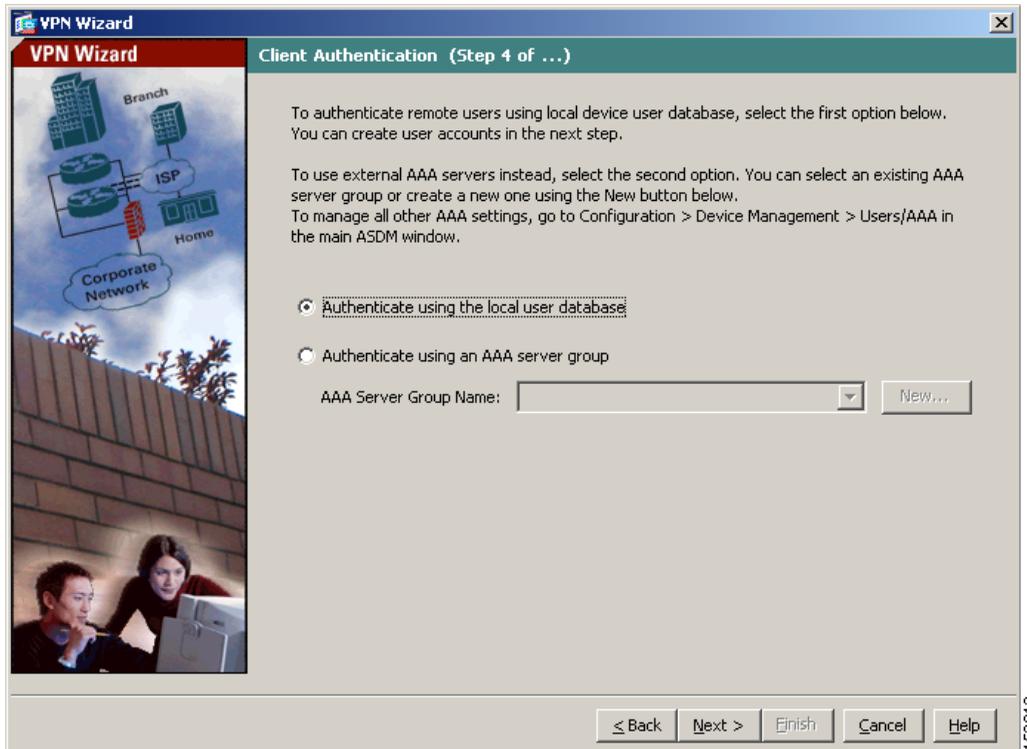
**ステップ 3** **Next** をクリックして続行します。

## ユーザ認証方式の指定

ユーザの認証は、ローカル認証データベース、または外部の Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントिंग) サーバを使用して実行できます (AAA サーバには RADIUS、TACACS+、SDI、NT、Kerberos、および LDAP があります)。

VPN Wizard の Step 4 で、次の手順に従います。

- 
- ステップ 1** 適応型セキュリティ アプライアンスにユーザ データベースを作成してユーザを認証するには、**Authenticate Using the Local User Database** オプション ボタンをクリックします。
- ステップ 2** 外部 AAA サーバ グループを使用してユーザを認証する場合は、次の手順に従います。
- a. **Authenticate Using an AAA Server Group** オプション ボタンをクリックします。
  - b. 事前設定されているサーバ グループを **Authenticate using an AAA Server Group** ドロップダウン リストから選択するか、**New** をクリックして新しい AAA サーバ グループを追加します。



**ステップ 3** Next をクリックして続行します。

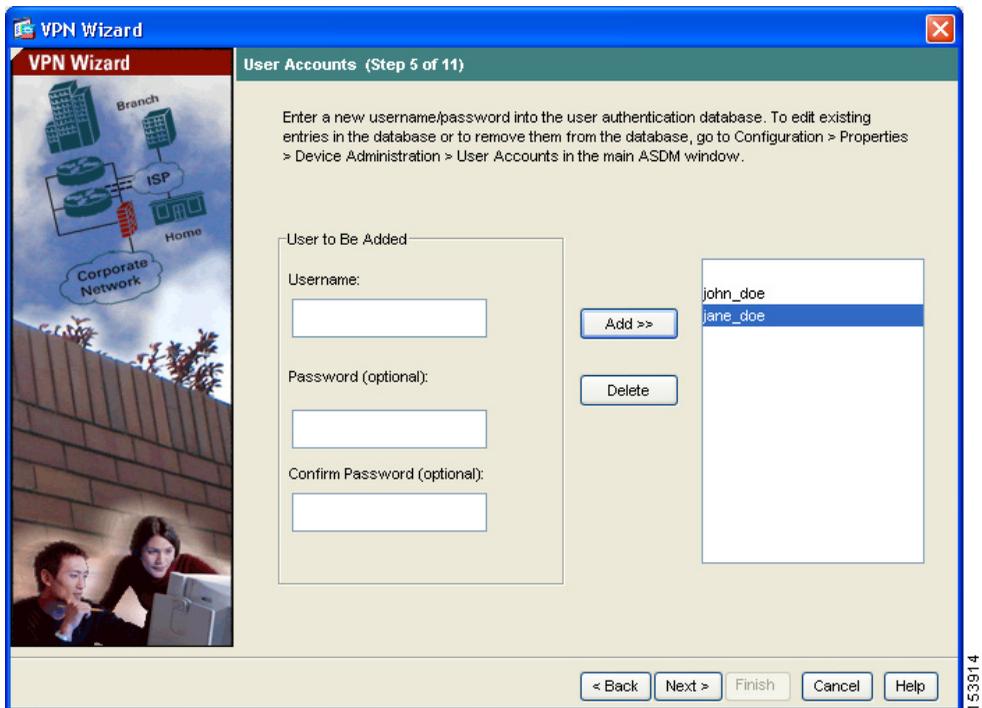
---

## (オプション) ユーザアカウントの設定

ローカル ユーザ データベースを使用してユーザを認証する場合、次の手順で新しいユーザアカウントを作成できます。ASDM 設定インターフェイスを使用して、後でユーザを追加することもできます。

VPN Wizard の Step 5 で、次の手順に従います。

- ステップ 1** 新しいユーザを追加するには、ユーザ名とパスワードを入力し、**Add** をクリックします。



- ステップ 2** 新しいユーザの追加が終了したら、**Next** をクリックして続行します。

## アドレス プールの設定

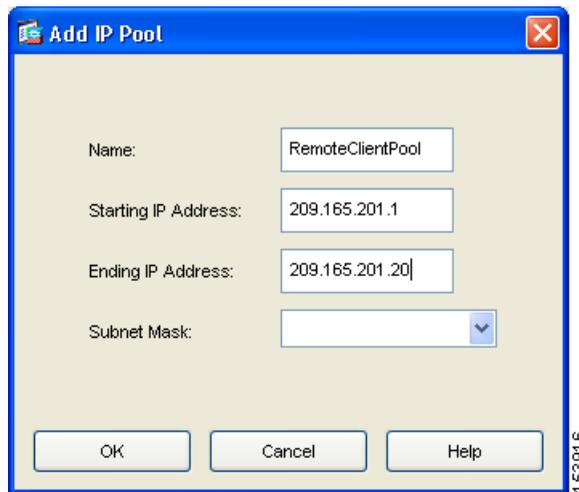
リモート クライアントがネットワークにアクセスするには、接続に成功したときにリモート VPN クライアントに割り当てられる可能性のある IP アドレスのプールを設定する必要があります。このシナリオでは、プールは 209.165.201.1 ~ 209.166.201.20 の範囲の IP アドレスを使用するように設定します。

VPN Wizard の Step 6 で、次の手順に従います。

**ステップ 1** プール名を入力するか、事前設定されているプールを Name ドロップダウン リストから選択します。

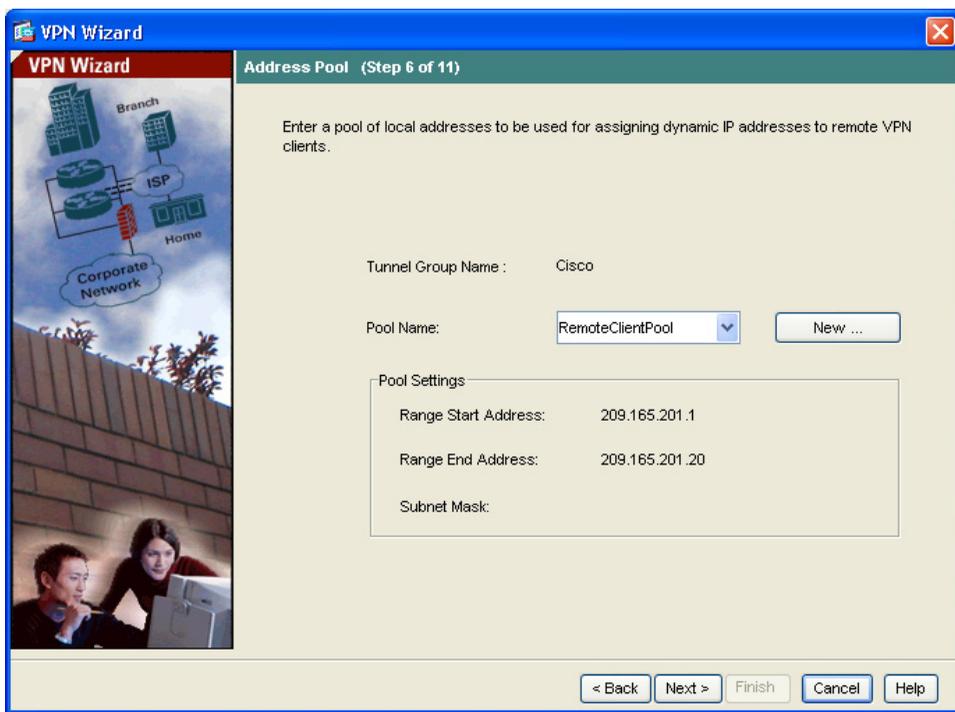
または、**New** をクリックして、新しいアドレス プールを作成します。

Add IP Pool ダイアログボックスが表示されます。



**ステップ 2** Add IP Pool ダイアログボックスで、次の内容を実行します。

- a. 範囲の開始 IP アドレスと終了 IP アドレスを入力します。
- b. (オプション) サブネット マスクを入力するか、Subnet Mask ドロップダウンリストから IP アドレス範囲のサブネットマスクを選択します。
- c. **OK** をクリックして、VPN Wizard の Step 6 に戻ります。



**ステップ 3** **Next** をクリックして続行します。

## クライアントアトリビュートの設定

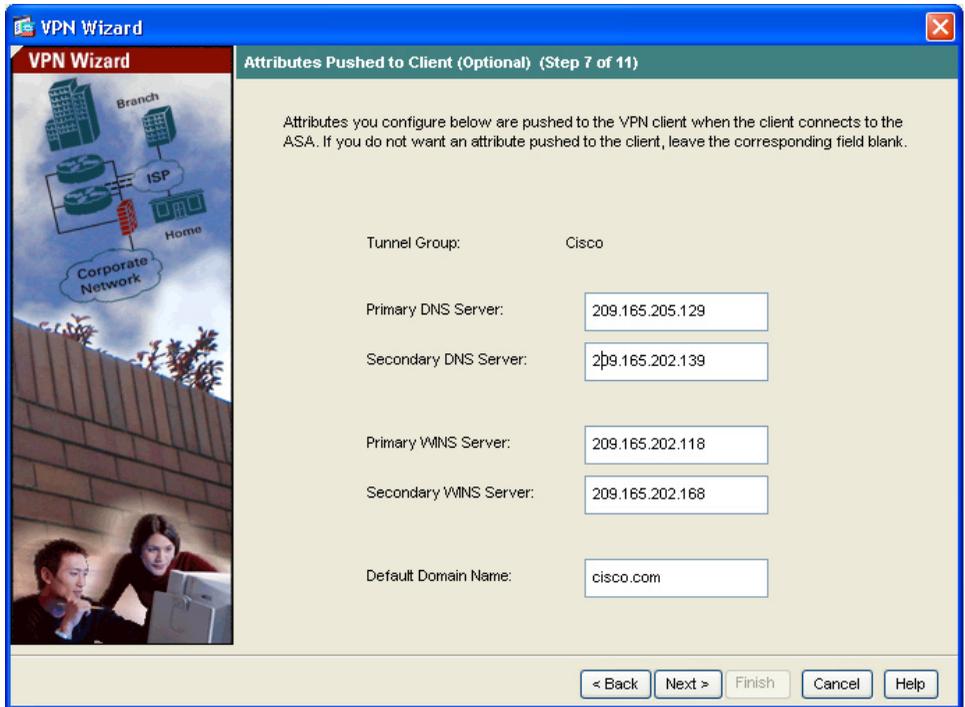
各リモートアクセスクライアントがネットワークにアクセスするには、使用する DNS サーバと WINS サーバ、デフォルトのドメイン名などの基本的なネットワーク設定情報が必要です。各リモートクライアントを個々に設定するのではなく、ASDM にクライアント情報を設定できます。接続が確立されると、適応型セキュリティアプライアンスは、この情報をリモートクライアントまたは Easy VPN ハードウェアクライアントに適用します。

必ず正しい値を指定してください。値が正しくない場合、リモートクライアントが解決に DNS 名を使用できない、または Windows ネットワーキングを使用できないという問題が発生します。

VPN Wizard の Step 7 で、次の手順に従います。

---

**ステップ 1** リモートクライアントに適用するネットワーク設定情報を入力します。



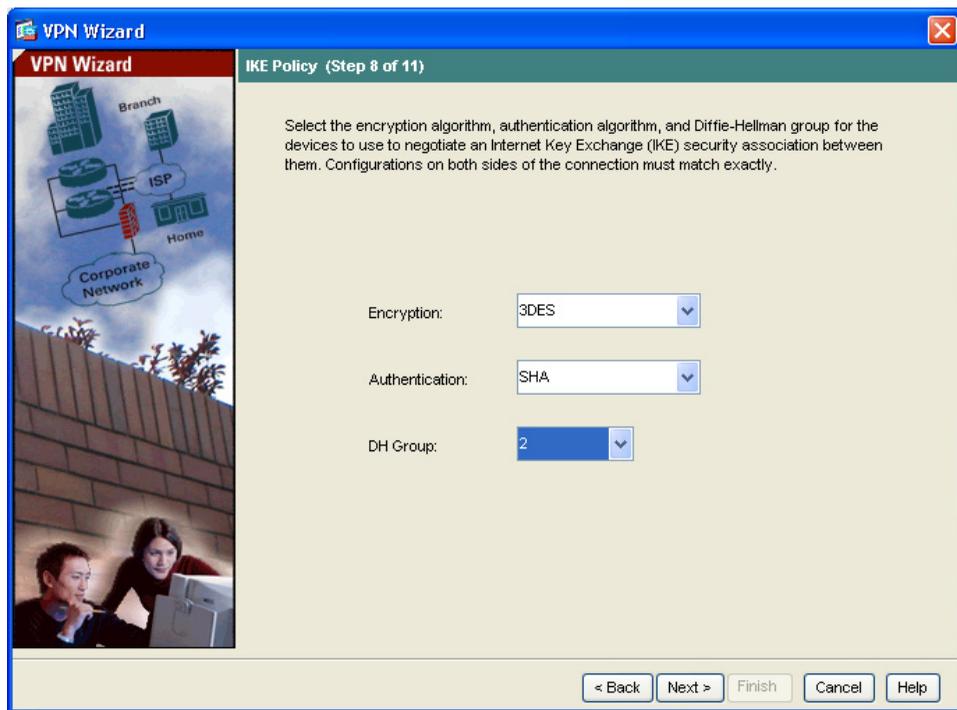
**ステップ 2** Next をクリックして続行します。

## IKE ポリシーの設定

IKE は、データを保護しプライバシーを保証する暗号化方式を含むネゴシエーションプロトコルで、ピアの ID を確認する認証方式でもあります。ほとんどの場合、ASDM のデフォルト値を使用すれば、十分にセキュアな VPN トンネルを確立できます。

VPN Wizard の Step 8 で IKE ポリシーを指定するには、次の手順に従います。

- ステップ 1** IKE セキュリティ アソシエーションにおいて適応型セキュリティ アプライアンスが使用する暗号化アルゴリズム (DES、3DES、または AES)、認証アルゴリズム (MD5 または SHA)、および Diffie-Hellman グループ (1、2、5、または 7) を選択します。

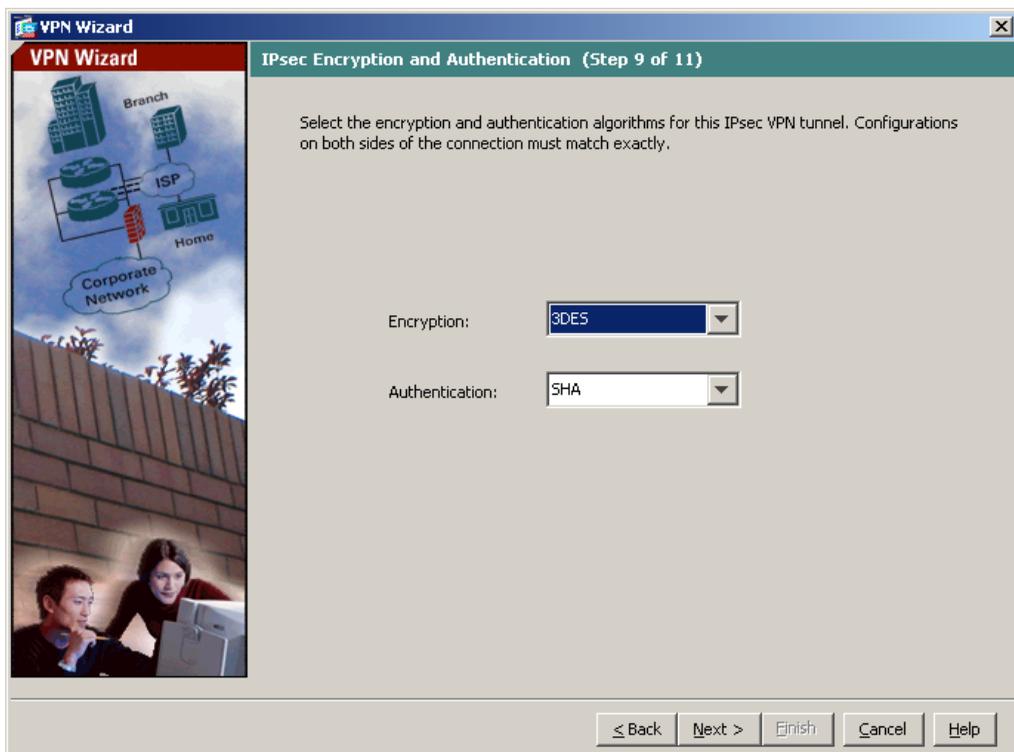


**ステップ 2** **Next** をクリックして続行します。

## IPsec Encryption パラメータ および Authentication パラメータの設定

VPN Wizard の Step 9 で、次の手順に従います。

**ステップ 1** 暗号化アルゴリズム (DES、3DES、または AES) および認証アルゴリズム (MD5 または SHA) をクリックします。



**ステップ 2** **Next** をクリックして続行します。

---

## アドレス変換の例外およびスプリット トンネリングの指定

スプリット トンネリングを使用すると、リモートアクセス IPsec クライアントは、パケットを条件によって、IPsec トンネル経由で送信すること（暗号化形式）や、ネットワーク インターフェイスに送信すること（テキスト形式）ができます。

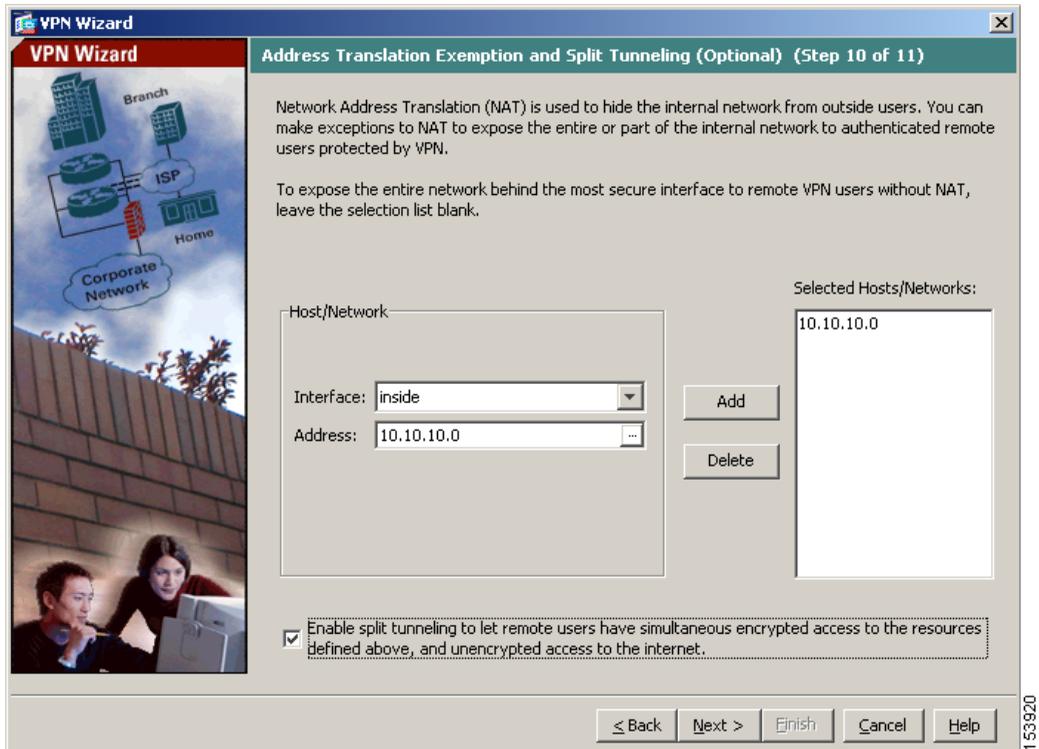
適応型セキュリティ アプライアンスは、Network Address Translation (NAT; ネットワーク アドレス変換) を使用して、内部 IP アドレスが外部に公開されないようにしています。認証されたリモート ユーザにアクセスを許可するローカル ホストおよびネットワークを特定することで、このネットワーク保護に例外を設定できます。

VPN Wizard の Step 10 で、次の手順に従います。

---

**ステップ 1** 認証されたリモート ユーザにアクセスを許可する内部リソースのリストに入れるホスト、グループ、およびネットワークを指定します。

Selected Hosts/Networks ペインのホスト、グループ、およびネットワークを動的に追加するには **Add**、動的に削除するには **Delete** をクリックします。



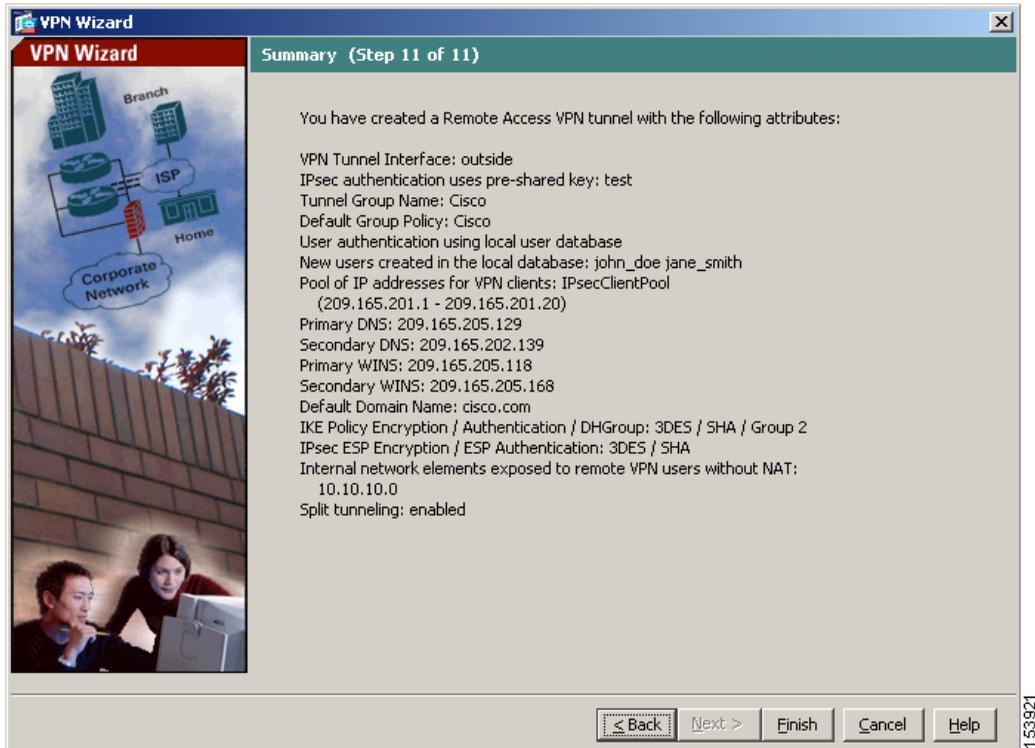
(注)

画面下部の **Enable Split Tunneling ...** チェックボックスをオンにすると、スプリット トンネリングがイネーブルになります。スプリット トンネリングを使用すると、設定したネットワークの外部のトラフィックは、暗号化された VPN トンネルを経由せずにインターネットに直接送信されます。

**ステップ 2** Next をクリックして続行します。

## リモートアクセス VPN 設定の確認

VPN Wizard の Step 11 で、新しい VPN トンネルの設定アトリビュートを確認します。表示される設定は次のようになります。



適切に設定されている場合は **Finish** をクリックして、適応型セキュリティアプライアンスに変更内容を適用します。

次にデバイスを起動するときに適用されるように、設定変更をスタートアップコンフィギュレーションに保存する場合は、**File** メニューから **Save** をクリックします。または、**ASDM** を終了するときに設定変更を半永久的に保存するように求められます。

設定変更を保存しない場合は、次にデバイスを起動するときに変更前の設定がそのまま適用されます。

---

## 次の作業

モバイル従業員またはテレワーカー向けの安全な接続用にエンドツーエンドの暗号化 VPN トンネルを確立するには、Cisco VPN クライアント ソフトウェアを入手します。

Cisco Systems VPN クライアントの詳細については、<http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html> を参照してください。

リモートアクセス VPN 環境だけに適応型セキュリティ アプライアンスを配置する場合は、これで初期設定が終了しました。さらに、次の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	『Cisco Security Appliance Command Line Configuration Guide』
日常的な運用について	『Cisco Security Appliance Command Reference』 『Cisco Security Appliance Logging Configuration and System Log Messages』

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の項では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

実行内容	参照先
DMZ 内の Web サーバを保護するための適応型セキュリティ アプライアンスの設定	第6章「シナリオ : DMZ 設定」
サイトツーサイト VPN の設定	第8章「シナリオ : サイトツーサイト VPN 設定」